



บทที่ 13

จริยธรรมและความปลอดภัย



บทที่ 13 จริยธรรมและความปลอดภัย

- ความหมายของจริยธรรม

- แบบแผนความประพฤติ หรือความมีสามัญสำนึกต่อสังคมในทางที่ดี
- ไม่มีกฎเกณฑ์ตายตัวขึ้นอยู่กับกลุ่มสังคมหรือการยอมรับในสังคมนั้นเป็นหลัก
- เกี่ยวข้องกับการคิดและตัดสินใจได้ว่าสิ่งไหน ควร-ไม่ควร ดี-ไม่ดี ถูก-ผิด



จริยธรรมกับกฎระเบียบ

- “**มีจริยธรรม**” มีสามัญสำนึกดี ประพฤติปฏิบัติดี ไม่ก่อให้เกิดผลเสียหายต่อสังคมโดยรวม
- “**ขาดจริยธรรม**” มีรูปแบบการประพฤติหรือปฏิบัติตนที่ไม่มีประโยชน์หรืออาจส่งผลไม่ดีต่อสังคม
- การควบคุมให้คนมีจริยธรรมที่ดี อาจใช้ข้อบังคับ กฎ หรือระเบียบของสังคมมาเป็นส่วนสนับสนุนให้เกิด “จริยธรรมที่ดี” ได้

จริยธรรมกับสังคมยุคสารสนเทศ

- ตั้งอยู่บนพื้นฐาน 4 ประเด็นคือ
 - ความเป็นส่วนตัว (Information Privacy)
 - ความถูกต้องแม่นยำ (Information Accuracy)
 - ความเป็นเจ้าของ (Information Property)
 - การเข้าถึงข้อมูล (Information Accessibility)

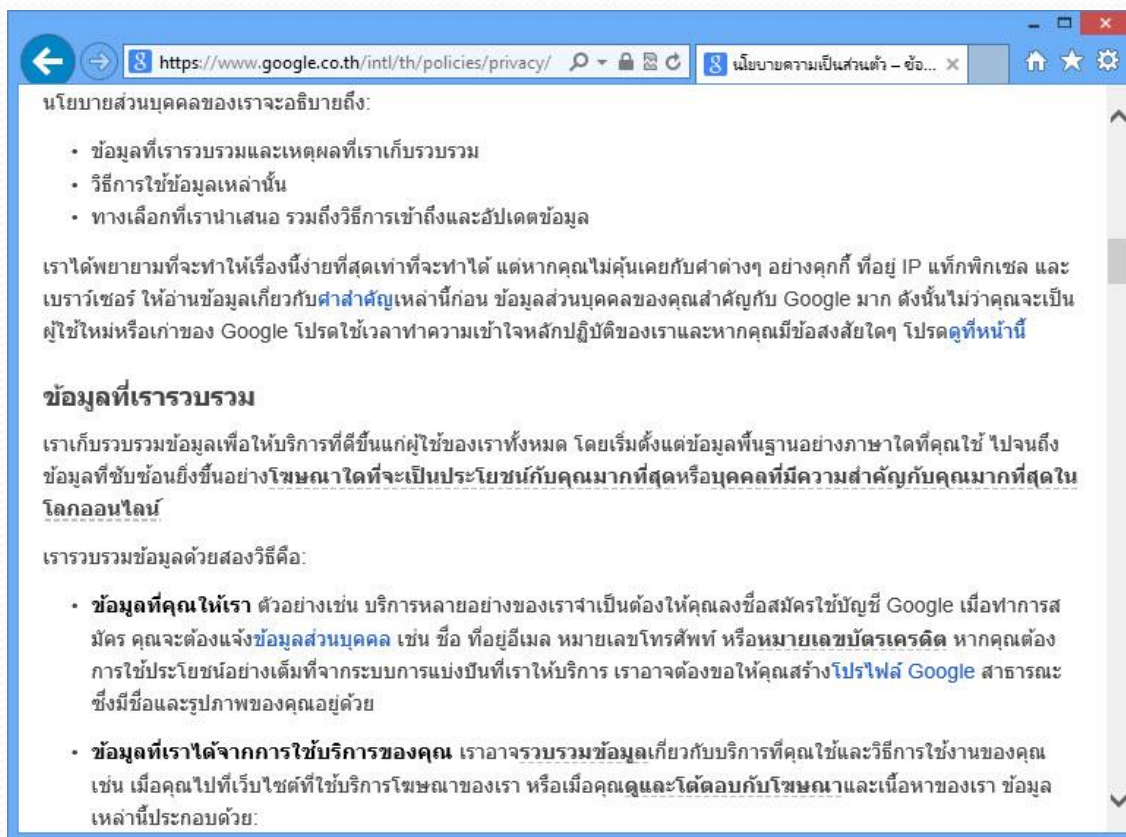




ความเป็นส่วนตัว (Information Privacy)

- ความเป็นส่วนตัว หมายถึง สิทธิส่วนตัวของบุคคล หน่วยงาน หรือองค์กร ที่จะคงไว้ซึ่งสารสนเทศที่มีอยู่ นั้น เพื่อตัดสินใจได้ว่าจะสามารถเปิดเผยให้ผู้อื่นนำไปใช้ประโยชน์ต่อหรือเผยแพร่ได้หรือไม่
- การละเมิดความเป็นส่วนตัว เช่น
 - ใช้โปรแกรมติดตามและพฤติกรรมผู้ที่ใช้งานบนเว็บไซต์
 - การเอาฐานข้อมูลส่วนตัว รวมถึงอีเมลล์ของสมาชิกส่งไปให้กับบริษัทผู้รับทำโฆษณา
 - ฯลฯ

ความเป็นส่วนตัว (ต่อ)



นโยบายส่วนบุคคลของเราจะอธิบายถึง:

- ข้อมูลที่เรารวบรวมและเหตุผลที่เราเก็บรวบรวม
- วิธีการใช้ข้อมูลเหล่านั้น
- ทางเลือกที่เรานำเสนอ รวมถึงวิธีการเข้าถึงและอัปเดตข้อมูล

เราได้พยายามที่จะทำให้อะไรที่ง่ายที่สุดเท่าที่จะทำได้ แต่หากคุณไม่คุ้นเคยกับหลายๆ อย่างคุณก็ ที่อยู่ IP แท็กพิกเซล และ เบรเวอเซอร์ ให้อ่านข้อมูลเกี่ยวกับ**คำสั่ง**เหล่านี้ก่อน ข้อมูลส่วนบุคคลของคุณสำคัญกับ Google มาก ดังนั้นไม่ว่าคุณจะเป็น ผู้ใช้ใหม่หรือเก่าของ Google โปรดใช้เวลาทำความเข้าใจหลักปฏิบัติของเราและหากคุณมีข้อสงสัยใดๆ โปรดดูที่**หน้า**

ข้อมูลที่เรารวบรวม

เราเก็บรวบรวมข้อมูลเพื่อให้บริการที่ดีขึ้นแก่ผู้ใช้ของเราทั้งหมด โดยเริ่มตั้งแต่ข้อมูลพื้นฐานอย่างภาษาใดที่คุณใช้ ไปจนถึง ข้อมูลที่ซับซ้อนยิ่งขึ้นอย่าง**โฆษณา**ใดที่จะเป็น**ประโยชน์**กับ**คุณมากที่สุด**หรือ**บุคคลที่มีความสำคัญ**กับ**คุณมากที่สุด**ใน**โลกออนไลน์**

เรารวบรวมข้อมูลด้วยสองวิธีคือ:

- **ข้อมูลที่คุณให้เรา** ตัวอย่างเช่น บริการหลายอย่างของเราจำเป็นต้องให้คุณลงชื่อสมัครใช้บัญชี Google เมื่อทำการสมัคร คุณจะต้องแจ้ง**ข้อมูลส่วนบุคคล** เช่น ชื่อ ที่อยู่อีเมล หมายเลขโทรศัพท์ หรือ**หมายเลขบัตรเครดิต** หากคุณต้องการใช้ประโยชน์อย่างเต็มที่จากระบบการแบ่งปันที่เราให้บริการ เราอาจต้องขอให้คุณสร้าง**โปรไฟล์ Google** สาธารณะ ซึ่งมีชื่อและรูปภาพของคุณอยู่ด้วย
- **ข้อมูลที่เราได้จากการใช้บริการของคุณ** เราอาจ**รวบรวมข้อมูล**เกี่ยวกับบริการที่คุณใช้และวิธีการใช้งานของคุณ เช่น เมื่อคุณไปที่เว็บไซต์ที่ใช้บริการโฆษณาของเรา หรือเมื่อคุณดูและโต้ตอบกับ**โฆษณา**และเนื้อหาของเรา ข้อมูลเหล่านี้ประกอบด้วย:

คำชี้แจงสิทธิส่วนบุคคลก่อนใช้บริการ



ความเป็นส่วนตัว (ต่อ)

- **ความเป็นส่วนตัวในยุคสังคมออนไลน์ (Social Network)**
 - เจ้าของข้อมูลตั้งใจเปิดเผยเรื่องราวส่วนตัว
 - ความเป็นส่วนตัวในยุคของเครือข่ายสังคมออนไลน์ถูกมองข้ามไปมาก
 - เหตุการณ์หรือกิจกรรมต่างๆถูกเปิดเผยแทบตลอดเวลา
 - ผู้ไม่ประสงค์ดีอาจคอยติดตามข้อมูลข่าวสารของเราได้
 - อาจเกิดอันตรายต่อทรัพย์สินและความมั่นคงของชีวิตได้



ความถูกต้องแม่นยำ (ต่อ)

- สารสนเทศที่น่าเสนอ ควรเป็นข้อมูลที่มีการกลั่นกรองและตรวจสอบความถูกต้อง และสามารถนำไปใช้ประโยชน์ได้ โดยไม่ส่งผลกระทบต่อผู้ใช้งาน
- ตัวอย่างเช่น แหล่งข่าวทางอินเทอร์เน็ต อาจนำเสนอเนื้อหาที่ไม่ได้กลั่นกรอง เมื่อนำไปตีความและเข้าใจว่าเป็นจริง จะทำให้เกิดความผิดพลาดได้
- ผู้ใช้งานสารสนเทศควรเลือกรับข้อมูลจากแหล่งที่น่าเชื่อถือ และตรวจสอบที่มาได้

ความถูกต้องแม่นยำ (ต่อ)



กรมวิทยาศาสตร์การแพทย์ ได้ข่าวลือย่น น้ำขวดพลาสติกเก็บในรถนานๆ ไม่ก่อสารพิษ ดื่มน้ำได้ หลังทดสอบไม่พบสารก่อมะเร็งตามข่าวในโลกออนไลน์



รายงานข่าวแจ้งว่า วานนี้ (2 มี.ย. 57) กรมวิทยาศาสตร์การแพทย์ กระทรวงสาธารณสุข (สธ.) นำโดย นพ.อภิชัย มงคล อธิบดี ใต้ออกมาเปิดเผยข้อมูล หลังมีข่าวลือในโลกออนไลน์ว่า การดื่มน้ำบรรจุขวดพลาสติกที่เก็บในหลังรถยนต์และจอดแช่กลางแดดนานๆ เสี่ยงต่อการเป็นโรคมะเร็งเต้านม และมะเร็งอื่นๆ เนื่องจากแสงแดดจะไปทำปฏิกิริยากับขวดพลาสติก จนเกิดมีสารไดออกซินปนเปื้อนมาด้วยนั้น ว่า ยังไม่มีหลักฐานทางวิทยาศาสตร์ยืนยันตรวจพบไดออกซินในพลาสติก และสารเคมีต่างๆ ละลายออกมาจากขวดพลาสติก ทั้งในสภาวะอุณหภูมิสูง หรือสภาวะการแช่แข็ง และจากการทดลองได้ผลยืนยันว่า ไม่พบสารประกอบกลุ่มไดออกซิน และพีซีบีที่ละลายออกมาในทุกตัวอย่าง ดังนั้นจึงอยากเตือนผู้บริโภคควรพิจารณาแหล่งของข่าวสารต่างๆ ที่ได้รับจากสื่อสังคมออนไลน์และตรวจสอบที่มาด้วยเพื่อให้ได้ข้อมูลที่ถูกต้องน่าเชื่อถือ

สำหรับ สารไดออกซิน (Dioxins) เป็นผลผลิตทางเคมีที่เกิดขึ้นโดยมิได้ตั้งใจ จากการเผาไหม้ที่ไม่สมบูรณ์ และกระบวนการเผาไหม้อุณหภูมิสูงทุกชนิด โดยมีแหล่งกำเนิดสำคัญของสารกลุ่มนี้คือกระบวนการผลิตเคมีภัณฑ์ที่มีสารคลอรีนเป็นองค์ประกอบ ซึ่งแม้ว่าขวดพลาสติกบางชนิดจะมีส่วนผสมของสารคลอรีน แต่อุณหภูมิของน้ำในขวดที่ถูกรังไว้หลังรถไม่ได้สูงมากพอที่จะทำให้เกิดสารไดออกซินขึ้นมาได้ และขวดชนิดดังกล่าวก็ไม่นิยมนำมาบรรจุน้ำสำหรับดื่มเช่นกัน

▲ ตัวอย่างข้อมูลที่แชร์ต่อกันไปทางอินเทอร์เน็ต ▲ ข่าวที่ออกมาชี้แจงความถูกต้องของเนื้อหาที่แชร์กัน



ความเป็นเจ้าของ (Information Property)

- สังคมยุคสารสนเทศมีการเผยแพร่ข้อมูลอย่างง่ายดาย มีเครื่องมือและอุปกรณ์สนับสนุนมากขึ้น
- ก่อให้เกิดการลอกเลียนแบบ ทำซ้ำ หรือละเมิดลิขสิทธิ์ (Copyright) โดยเจ้าของผลงานได้รับผลกระทบทั้งทางตรงและทางอ้อม
- ตัวอย่างเช่น การทำซ้ำหรือผลิตซ้ำดีเพลง และโปรแกรมละเมิดลิขสิทธิ์

ความเป็นเจ้าของ (ต่อ)

การแสดงความ
เป็นเจ้าของข้อมูล
บนเว็บไซต์ของ
ผู้ให้บริการ

Microsoft NOKIA

Home

ข้อกำหนดในการใช้งานเว็บไซต์

ข้อกำหนดในการใช้งานเว็บไซต์

การเข้าถึงหน้าอุปกรณ์และบริการ (ซึ่งหมายถึงและเชื่อมโยงกับข้อกำหนดเหล่านี้) หมายถึงว่าคุณได้ยอมรับข้อตกลงดังต่อไปนี้แล้ว โปรดทราบว่าหากคุณไม่ยอมรับข้อตกลงต่อไปนี้ คุณจะไม่สามารถได้รับอนุญาตให้เข้าใช้งานเว็บไซต์นี้

เนื้อหาของหน้าเว็บของเว็บไซต์เหล่านี้เป็น Copyright © Microsoft Mobile Oy 2014 ("Microsoft") รวมถึงสิทธิ์ต่างๆ ที่ไม่ได้ปรากฏโดยชัดเจนในนี้ยังคงมีการสงวนไว้ ห้ามมีการทำซ้ำ การโอน การแจกจ่าย หรือการจัดเก็บบางส่วนหรือทั้งหมดของเนื้อหาไม่ว่าจะอยู่ในรูปแบบใด โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจาก Nokia ก่อน เว้นแต่เป็นไปตามข้อตกลงที่จะได้กล่าวต่อไป Microsoft ยินยอมให้คุณท่องไปบนหน้าบนเว็บไซต์เหล่านี้จากคอมพิวเตอร์ของคุณหรือสิ่งพิมพ์เนื้อหาจากหน้าเว็บเหล่านี้เพื่อการใช้ส่วนตัว และไม่นำไปแพร่กระจายซ้ำ โดยไม่ได้รับการยินยอมเป็นลายลักษณ์อักษรจาก Microsoft เอกสารแต่ละรายการบนหน้าเว็บของเราอาจมีข้อกำหนดเพิ่มเติมระบุอยู่ในเอกสารเหล่านั้น

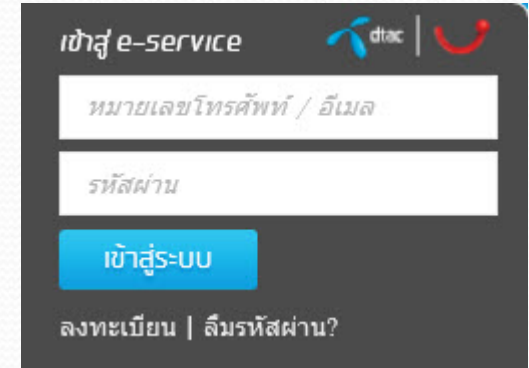
ความเป็นเจ้าของ (ต่อ)

- การอนุญาตให้ใช้งาน (License)

- **Copyright** © หากมีข้อความนี้จะหมายถึงสงวนลิขสิทธิ์ ห้ามนำเอาผลงานไปใช้หรือทำซ้ำโดยเด็ดขาด นอกจากนี้การขออนุญาตอย่างเป็นทางการจากเจ้าของผลงานก่อน
- **Creative Commons** (CC) หรือเรียกว่า **Copyleft** (∞) (เพื่อให้สอดคล้องกับคำว่า Copyright) เป็นการอนุญาตให้นำผลงานไปใช้ต่อยอดได้ในบางกรณี
- **Public Domain** (∅) เป็นผลงานที่ไม่สงวนลิขสิทธิ์ จะนำไปใช้งานอะไรก็ได้ แต่ในทางปฏิบัติควรให้เครดิตเจ้าของผลงานกำกับไว้ด้วยเสมอ

การเข้าถึงข้อมูล (Information Accessibility)

- ผู้ดูแลระบบ จะเป็นผู้ที่กำหนดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้แต่ละคน เช่น เข้าถึงข้อมูลโดยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
- การเข้าถึงข้อมูลนั้นสามารถให้บริการและเข้าถึงได้หลากหลายวิธี เช่น
 - ภาพถ่ายหรือรูปภาพที่ปรากฏบนเว็บไซต์ ควรมีคำอธิบายภาพ (Attribute หรือ Alt) เพื่อสื่อความหมายไว้ด้วยว่าเป็นภาพอะไร
 - สร้างชื่อลิงก์ (Link) ที่มีความหมายในตัว เพื่อบอกให้ผู้ใช้ทราบ



การเข้าถึงข้อมูล (Information Accessibility) (ต่อ)

- ระบบล็อกสองขั้นตอน (Two-Step Verification)
 - บางระบบมีบริการ “ล็อกสองขั้นตอน” เพื่อป้องกันผู้ไม่หวังดีแอบล็อกอินเข้าใช้บัญชีส่วนตัว
 - ตัวอย่างเช่น บัญชี Gmail ของ Google หรือ บัญชี Apple ID บนสมาร์ทโฟนระบบ iOS โดยจะผูกเบอร์โทรศัพท์ไว้กับบัญชีอีเมล
 - ถ้ามีการล็อกอินเข้าระบบจากคอมพิวเตอร์ หรืออุปกรณ์เครื่องอื่นที่เราไม่เคยใช้ ระบบจะส่ง SMS แจ้งรหัสพิเศษมายังโทรศัพท์

การเข้าถึงข้อมูล (Information Accessibility) (ต่อ)

Two-step verification for Apple ID.

Two-step verification will require you to verify your identity using one of your devices before you can make changes to your account or make an iTunes or App Store purchase from a new device.



You enter your Apple ID and password as usual.

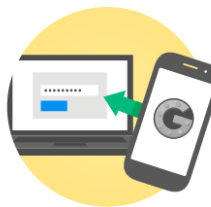
We send a verification code to one of your devices.

You enter the code to verify your identity and complete sign in.

▲ <https://appleid.apple.com>

Google

การลงชื่อเข้าใช้ด้วยการยืนยันแบบสองขั้นตอน



การลงชื่อเข้าใช้จะแตกต่างกัน

คุณต้องใช้รหัสยืนยัน: หลังจากป้อนรหัสผ่าน คุณจะต้องป้อนรหัสที่ คุณจะได้รับผ่านทางข้อความ การโทร หรือแอปพลิเคชันมือถือของเรา



ใช้งานอย่างง่ายดาย

หนึ่งครั้งต่อหนึ่งคอมพิวเตอร์ หรือทุกครั้ง: ระหว่างที่ลงชื่อเข้าใช้ คุณสามารถแจ้งให้เราไม่ต้องขอให้คุณป้อนรหัสอีกครั้งบนคอมพิวเตอร์ที่ต้องการได้



ช่วยป้องกันบุคคลอื่น

คุณจะมีคงได้รับการคุ้มครอง: เราจะขอรหัสมือถือคุณ (หรือบุคคลอื่น) พยายามลงชื่อเข้าใช้บัญชีของคุณจากคอมพิวเตอร์เครื่องอื่น

การยืนยันแบบสองขั้นตอน

ป้องกันบุคคลที่ไม่หวังดีให้ห่างจากบัญชีของคุณโดยใช่ที่รหัสผ่าน และโทรศัพท์ของคุณ

เริ่มการตั้งค่า »

เรียนรู้เพิ่มเติม

▲ <https://accounts.google.com/SMSAuthConfig>

อาชญากรรมคอมพิวเตอร์ (Computer Crime)

- การลักลอบนำเอาข้อมูลไปใช้โดยไม่ได้รับอนุญาต รวมถึงการสร้างความเสียหายต่อบุคคลและสังคมโดย “ผู้ไม่ประสงค์ดี” เกิดขึ้นจากการขาด “จริยธรรมที่ดี”
- บางกรณีถือว่าเป็นการกระทำที่ผิดกฎหมาย ซึ่งมีบทลงโทษแตกต่างกันไป
- ตัวอย่างของอาชญากรรมคอมพิวเตอร์ เช่น
 - การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต
 - การขโมยและทำลายอุปกรณ์
 - การขโมยโปรแกรมคอมพิวเตอร์
 - การก่อวินาศกรรมด้วยโปรแกรมประสงค์ร้าย
 - การก่อวินาศกรรมระบบด้วยสไปยาแวร์
 - การก่อวินาศกรรมด้วยสแปมเมลล์
 - การหลอกลวงเหยื่อเพื่อล้วงเอาข้อมูลส่วนตัว

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต

- อาชญากรรมที่เกี่ยวข้องกับการลักลอบหรืออ่านข้อมูลและนำไปใช้โดยไม่ได้รับอนุญาต
- เช่น การลักลอบเข้าไปแก้ไขข้อมูลเว็บเพจหน้าแรกขององค์กร
- กลุ่มคนที่เกี่ยวข้อง เช่น
 - แฮกเกอร์ (Hacker)
 - แครกเกอร์ (Cracker)
 - สคริปต์คิดดี (Script Kiddy)



ตัวอย่างการเข้าไปเปลี่ยนแปลงข้อมูล
เว็บเพจหน้าแรก แทนที่หน้าเว็บเพจเดิม



การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- แฮกเกอร์ (Hacker)
 - เป็นกลุ่มคนที่มีความรู้ทางด้านคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เป็นอย่างดี
 - บางคนอาจไม่ได้มีเจตนามุ่งร้ายต่อข้อมูล แต่ทำเพื่อต้องการทดสอบความรู้ของตนเอง นิยมเรียกคนกลุ่มนี้ว่า *คนหมวกขาว* หรือ *White Hat*



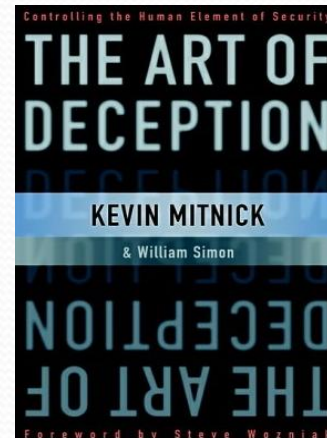
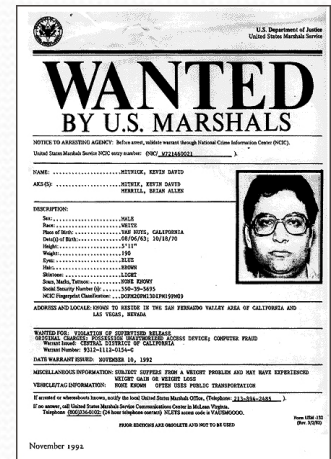
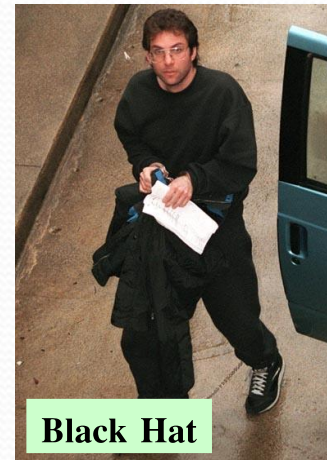
การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- แครกเกอร์ (Cracker)

- เป็นกลุ่มคนที่มีความรู้ความสามารถเช่นเดียวกับกลุ่มแฮกเกอร์
- มุ่งทำลายระบบหรือลักลอบนำเอาข้อมูลนั้นไปแก้ไข เปลี่ยนแปลง หรือทำลายทิ้ง
- มักเรียกว่าเป็น *กลุ่มคนหมวกดำ* หรือ *Black Hat*
- มีเจตนาจงใจให้ข้อมูลเกิดความเสียหายมากกว่าแฮกเกอร์

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- เควิน มิตนิก (Kevin Mitnick)
- บุคคลที่เป็นทั้งแฮกเกอร์และแครกเกอร์ในคนเดียว
- ขณะวัยรุ่นได้ใช้ความรู้ของตัวเองก่อความเสียหายให้กับหน่วยงานอื่นๆ
- ปัจจุบันหันมาให้ความรู้เกี่ยวกับระบบรักษาความปลอดภัยบนเครือข่ายแทน



การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- **สคริปต์คิตตี้** (Script Kiddy)

- มักเป็นคนอยากรู้ อยากเห็น ไม่จำเป็นต้องมีความรู้เกี่ยวกับการเจาะเข้าระบบมากนัก
- มีการแลกเปลี่ยนโปรแกรมหรือสคริปต์ (Scripts) ที่มีคนเขียนและนำออกมาเผยแพร่ให้ทดลองใช้กัน
- อาศัยโปรแกรมหรือเครื่องมือบางอย่างที่หามาได้ เช่น การแฮกอีเมล การขโมยรหัสผ่านของผู้อื่น หรือการใช้โปรแกรมก่อความเสียหาย

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- การลักลอบดักข้อมูลด้วยวิธี **Skimming** เป็นวิธีการที่ผู้ร้ายใช้โจรกรรมข้อมูล เช่น
 - นำอุปกรณ์อ่านข้อมูลขนาดเล็กไปแอบติดตั้งไว้ตามตู้ ATM เพื่อขโมยรหัส
 - ใช้เครื่อง Skimmer แอบดักข้อมูลบัตรเครดิต



▲ ปุ่มกดปลอมเพื่อแอบเก็บรหัสบัตร ATM



การขโมยและทำลายอุปกรณ์

- เกิดจากการไม่รอบคอบ และวางอุปกรณ์ไว้ในบริเวณที่เสี่ยงต่อการโจรกรรมได้ง่าย
- อาจเกิดจากบุคคลภายนอกหรือภายในองค์กร
- ควรมีการติดตั้งอุปกรณ์ป้องกันและรักษาความปลอดภัย ตรวจสอบการเข้าออกของบุคคลที่มาติดต่อ รวมถึงวางมาตรการในการใช้อุปกรณ์อย่างเข้มงวด





การขโมยโปรแกรมคอมพิวเตอร์

- อาชญากรรมที่เกี่ยวข้องกับการขโมยเอาข้อมูลโปรแกรม รวมถึงการคัดลอกโปรแกรมโดยผิดกฎหมาย
- สามารถทำซ้ำได้ง่าย ก่อให้เกิดความเสียหายกับบริษัทผู้ผลิต
- ลักลอบทำซ้ำข้อมูลโปรแกรม และนำออกวางจำหน่ายแทนที่โปรแกรมต้นฉบับจริง
- กลุ่มผู้ผลิตมีการออกกฎควบคุมการใช้ซอฟต์แวร์ และรวมกลุ่มกันเรียกว่า *BSA (Business Software Alliance)*

การขโมยโปรแกรมคอมพิวเตอร์ (ต่อ)

- **กลุ่ม BSA** (Business Software Alliance)

- คือกลุ่มพันธมิตรธุรกิจซอฟต์แวร์
- มีเครือข่ายครอบคลุมอยู่มากกว่า 80 ประเทศทั่วโลก
- จัดตั้งขึ้นเพื่อควบคุมและดูแลเรื่องการละเมิดลิขสิทธิ์
- รวมถึงการทำความเข้าใจกับผู้บริโภคให้ตระหนักถึงการใช้งานโปรแกรมที่ถูกต้อง





การก่อกรรบบด้วยโปรแกรมประสงค์ร้าย

- เป็นการใช้โปรแกรมที่มุ่งเน้นก่อกรรบบและทำลายระบบข้อมูลคอมพิวเตอร์
- สร้างความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์เป็นอย่างมาก
- กลุ่มโปรแกรมประสงค์ร้ายต่างๆ มีดังนี้
 - ไวรัสคอมพิวเตอร์ (Computer Virus)
 - เวิร์มหรือหนอนอินเทอร์เน็ต (Worm)
 - ม้าโทรจัน (Trojan horses)



การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- **ไวรัสคอมพิวเตอร์ (Computer Virus)**
 - เขียนโดยนักพัฒนาโปรแกรมที่มีความชำนาญเฉพาะด้าน
 - การทำงานจะอาศัยคำสั่งที่เขียนขึ้นภายในตัวโปรแกรมเพื่อกระจายไปยังเครื่องคอมพิวเตอร์เป้าหมาย
 - แพร่กระจายโดยอาศัยคนกระทำการอย่างใดอย่างหนึ่งกับพาหะที่โปรแกรมไวรัสนั้นแฝงตัวอยู่ เช่น รันโปรแกรม อ่านอีเมลล์ เปิดดูเว็บเพจ หรือเปิดไฟล์ที่แนบมา

การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- **เวิร์ม** หรือหนอนอินเทอร์เน็ต (Worm)
 - เป็นโปรแกรมที่มีความรุนแรงกว่าไวรัสคอมพิวเตอร์
 - จะทำลายระบบทรัพยากรคอมพิวเตอร์ให้มีประสิทธิภาพลดลง และไม่อาจทำงานต่อไปได้
 - การทำงานจะตรวจสอบเพื่อโจมตีหาเครื่องเป้าหมายก่อน จากนั้นจะวิ่งเจาะเข้าไปเอง
 - ลักษณะเด่นคือ สามารถทำสำเนาซ้ำตัวเองได้อย่างมหาศาลภายในเวลาเพียงไม่กี่นาที

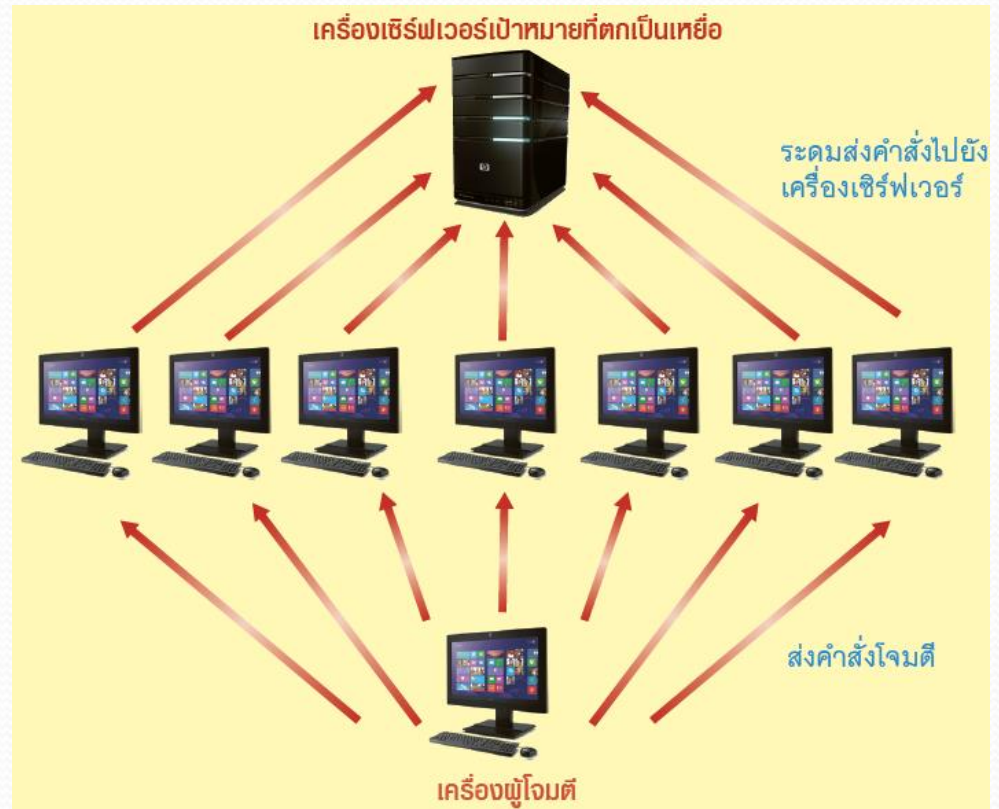
การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- **ม้าโทรจัน** (Trojan horses)
 - ทำงานโดยอาศัยการฝังตัวอยู่ในระบบคอมพิวเตอร์เครื่องนั้น และจะไม่แพร่กระจายตัว
 - โปรแกรมจะถูกตั้งเวลาการทำงาน หรือควบคุมการทำงานระยะไกลจากผู้ไม่ประสงค์ดี เพื่อเข้ามาทำงานยังเครื่องคอมพิวเตอร์เป้าหมายได้
 - ตัวอย่างเช่น แสร้งทำเป็นโปรแกรมยูทิลิตี้ให้ใช้งาน แต่แท้จริงคือโปรแกรมอันตราย เมื่อถึงเวลา ก็จะทำงานบางอย่างทันที

การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- ตัวอย่างการโจมตีเครื่องคอมพิวเตอร์ด้วย DoS (Denial of Service)

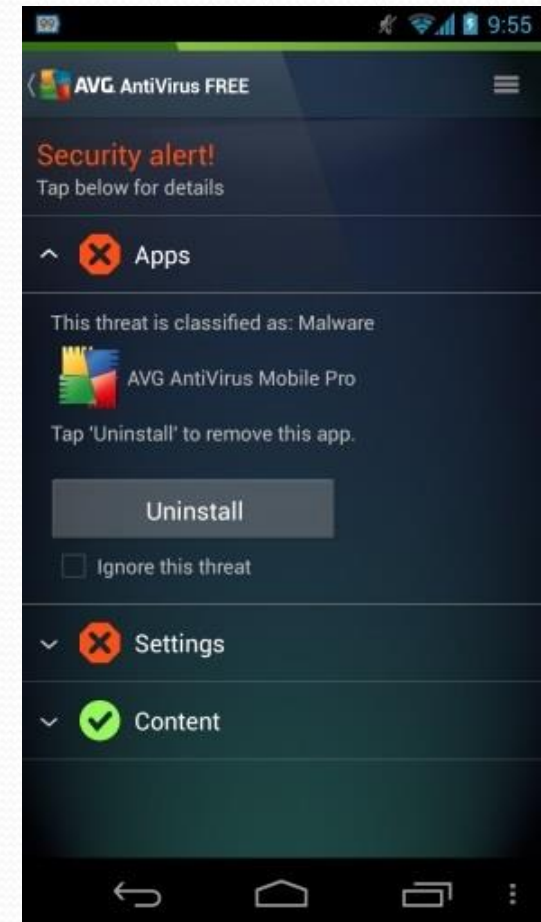
- มุ่งโจมตีเครื่องคอมพิวเตอร์เป้าหมายด้วยการส่งข้อมูลจำนวนมาก เพื่อให้เครื่องดังกล่าวไม่สามารถให้บริการอะไรได้เลย (Denial of Service)
- เรียกวิธีการโจมตีเหล่านี้ว่า *DoS Attack*



การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- ตัวอย่างแอปพลิเคชันปลอม/ขยะบนมือถือ

- แอปพลิเคชันประเภทคีย์บอร์ด ซึ่งคอยดักจับข้อมูลส่วนตัวที่พิมพ์ผ่านคีย์บอร์ด (Keyboard Logger) เช่น Username, Password หรือหมายเลขบัตรเครดิต
- แอปพลิเคชันสแกนไวรัส โดยแจ้งรายละเอียดว่าจะตรวจหาไวรัสบนเครื่อง แต่กลับขโมยข้อมูล SMS บนมือถือเครื่องนั้นส่งไปยังแฮกเกอร์





การก่อกวนระบบด้วยสปายแวร์ (Spyware)

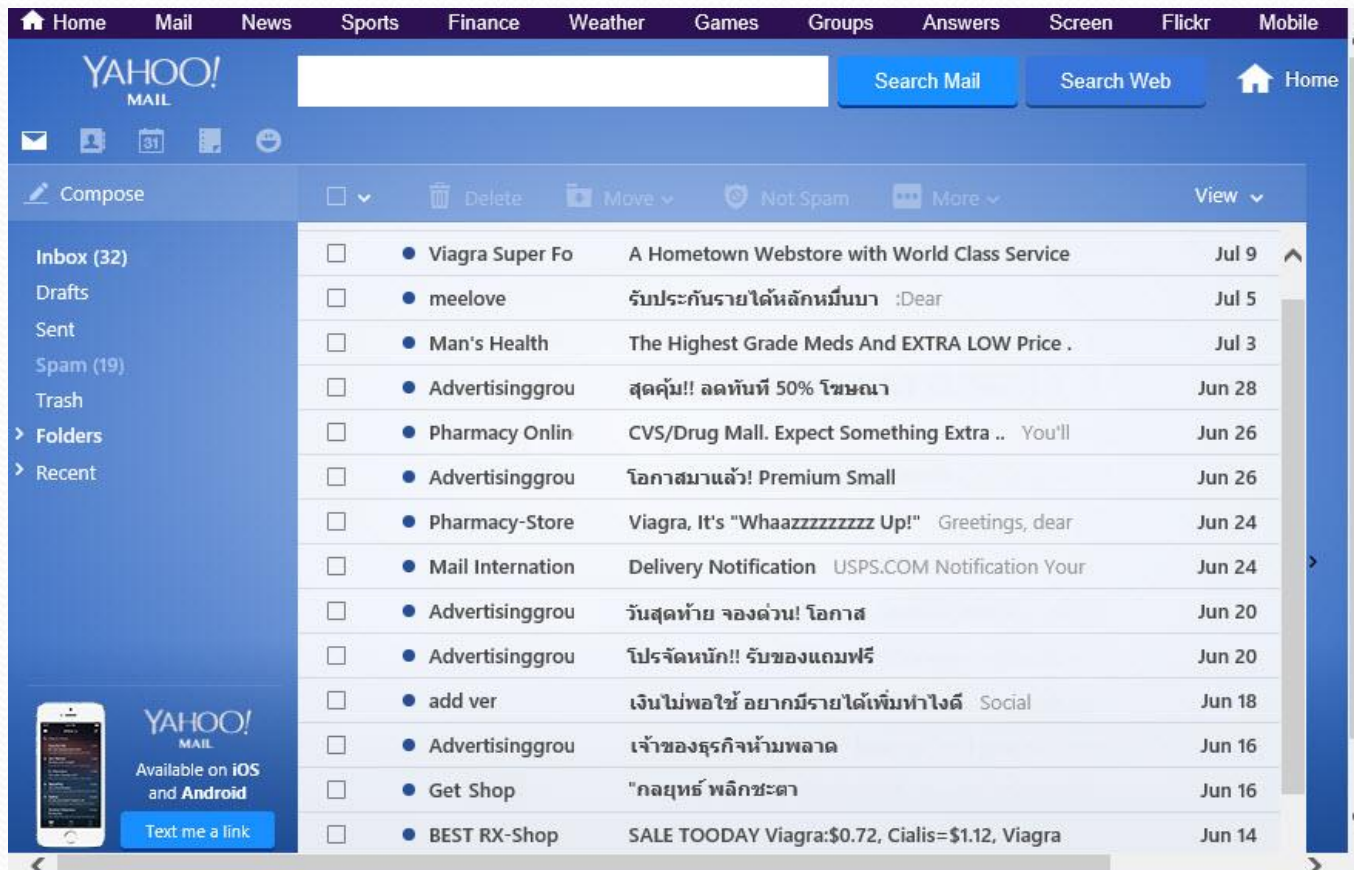
- **สปายแวร์** เป็นโปรแกรมประเภทสกดรอยข้อมูล
- ไม่ได้มีความร้ายแรงต่อคอมพิวเตอร์ เพียงแต่อาจทำให้เกิดความน่ารำคาญ
- โดยปกติมักแฝงตัวอยู่กับเว็บไซต์บางประเภท รวมถึงโปรแกรมที่แจกให้ใช้งานฟรีทั้งหลาย
- บางโปรแกรมสามารถควบคุมการเชื่อมต่ออินเทอร์เน็ต แทรกโฆษณาหรือเปลี่ยนหน้าแรกของบราวเซอร์ได้



การก่อกวนระบบด้วยสแปมเมลล์ (Spam Mail)

- สแปมเมลล์ คือรูปแบบของอีเมลที่ผู้รับไม่ต้องการอ่าน
- วิธีการก่อกวนจะอาศัยการส่งอีเมลแบบหว่านแห และส่งต่อให้กับผู้รับจำนวนมาก
- อาจถูกก่อกวนโดยแฮกเกอร์ หรือเกิดจากการถูกสะกดรอยด้วยโปรแกรมประเภทสปายแวร์
- ส่วนมากเป็นเมลล์ประเภทเชิญชวนให้ซื้อสินค้าหรือเลือกใช้บริการของเว็บไซต์นั้นๆ

การก่อกวนระบบด้วยสแปมเมลล์ (ต่อ)



The screenshot displays the Yahoo! Mail interface with a list of 15 emails in the inbox. The interface includes a navigation bar at the top with links for Home, Mail, News, Sports, Finance, Weather, Games, Groups, Answers, Screen, Flickr, and Mobile. Below the navigation bar is the Yahoo! Mail logo and search buttons for 'Search Mail' and 'Search Web'. The left sidebar shows folders like 'Inbox (32)', 'Drafts', 'Sent', 'Spam (19)', 'Trash', 'Folders', and 'Recent'. The main area shows a list of emails with columns for checkboxes, sender names, subject lines, and dates. The emails are predominantly spam, with subjects like 'Viagra Super Fo', 'meelove', 'Man's Health', 'Advertisinggrou', 'Pharmacy Onlin', 'Pharmacy-Store', 'Mail Internation', 'add ver', 'Get Shop', and 'BEST RX-Shop'. The dates range from Jun 14 to Jul 9.

Sender	Subject	Date
Viagra Super Fo	A Hometown Webstore with World Class Service	Jul 9
meelove	รับประกันรายได้หลักหมื่นบาท :Dear	Jul 5
Man's Health	The Highest Grade Meds And EXTRA LOW Price .	Jul 3
Advertisinggrou	สุดคุ้ม!! ลดทันที 50% โฆษณา	Jun 28
Pharmacy Onlin	CVS/Drug Mall. Expect Something Extra .. You'll	Jun 26
Advertisinggrou	โอกาสมาแล้ว! Premium Small	Jun 26
Pharmacy-Store	Viagra, It's "Whaazzzzzzzz Up!" Greetings, dear	Jun 24
Mail Internation	Delivery Notification USPS.COM Notification Your	Jun 24
Advertisinggrou	วันสุดท้าย จองด่วน! โอกาส	Jun 20
Advertisinggrou	โปรจัดหนัก!! รับของแถมฟรี	Jun 20
add ver	เงินไม่พอใช้ อยากมีรายได้เพิ่มทำไงดี Social	Jun 18
Advertisinggrou	เจ้าของธุรกิจห้ามพลาด	Jun 16
Get Shop	"กลยุทธ์ พลิกชะตา	Jun 16
BEST RX-Shop	SALE TODAY Viagra:\$0.72, Cialis=\$1.12, Viagra	Jun 14

การหลอกลวงเหยื่อเพื่อล้วงเอาข้อมูลส่วนตัว

- เป็นการหลอกลวงเพื่อล้วงข้อมูลส่วนตัว เช่น รายละเอียดหมายเลขบัตรเครดิต ชื่อผู้ใช้ หรือรหัสผ่านสำหรับใช้งานบนเว็บไซต์ โดยใช้กลวิธีต่างๆ เช่น
 - **Phishing** หลอกให้คลิกลิงก์ไปยังเว็บปลอม โดยใช้ข้อความที่เขียนขึ้นมาเอง หลอกลวงให้เหยื่อตายใจและหลงเชื่อกรอกข้อมูลส่วนตัวในเว็บปลอมนั้น
 - **Pharming** เป็นการเข้าโจมตีเซิร์ฟเวอร์ของเว็บไซต์ที่ตกเป็นเหยื่อ เพื่อเปลี่ยนแปลงค่าจากเครื่องเซิร์ฟเวอร์โดยตรง (DNS Hijacking หรือ DNS Redirection) โดยแก้ไขให้ DNS Server ไปเรียกลิงก์ของเว็บปลอมที่ผู้โจมตีสร้างขึ้น เมื่อมีผู้ใช้งานเรียกใช้เว็บไซต์ที่ถูกโจมตี ก็จะถูกส่งต่อไปยังเว็บปลอมโดยไม่รู้ตัว
- ** ผู้ใช้งานควรสังเกตชื่อ URL ว่าเรียกไปยังเว็บไซต์ที่ถูกต้อง ก่อนจะกรอกข้อมูลส่วนตัว*

ตัวอย่าง Phishing

ปรับปรุงล่าสุด 23 พฤษภาคม 2557

แจ้งเตือน โปรแกรมโทรจัน/สไปยาแวร์* จาก SMS ปลอมและอีเมลปลอม

ห้ามคลิก ห้ามกรอกเบอร์โทรศัพท์ ห้ามติดตั้ง Application บนโทรศัพท์มือถือ/Smartphone



เรียน ผู้ใช้บริการ

เรามีการพัฒนาและปรับปรุงระบบการให้บริการออนไลน์อย่างต่อเนื่อง เป็นความพยายามของเราที่จะทำให้ขั้นตอนการจัดการทางการเงินของผู้ใช้บริการมีความรวดเร็ว สะดวก และมีประสิทธิภาพยิ่งขึ้น. ความสำคัญลำดับแรกของเราคือการยังคงไว้ซึ่งบริการสำหรับลูกค้าในระดับสูง ด้วยการปฏิบัติตามความต้องการในด้านคุณภาพและความปลอดภัย.

ในปัจจุบัน, อาชญากรไซเบอร์ได้มีการใช้วิธีการที่หลากหลายเพื่อข้อความ SMS ขณะ แต่การป้องกันกับประสิทธิภาพน้อย ดังนั้น เพื่อความปลอดภัยอย่างยังคงข้อมูลทางการเงินของท่าน เราได้ทำการเพิ่มลำดับขั้นของการรักษาความปลอดภัย ด้วยการรับรองความปลอดภัยส่วนบุคคลสำหรับบริการในโทรศัพท์มือถือของคุณ.

มีขั้นตอนการทำงานอย่างไร.

การรับรองนี้จะติดตั้งในอีเมลของคุณโดยเฉพาะ ซึ่งมีติดตั้งในมือถือของท่านแล้ว ระบบจะทำการตรวจสอบ และประมวลผลขั้นการดำเนินการส่ง SMS ของเรา ซึ่งจะทำให้ SMS ขณะ ไม่สามารถเข้ามาถึงมือถือของคุณได้ และยังมีเป็นการช่วยลดความสามารถในการปลอมแปลงข้อความของคุณอีกด้วย

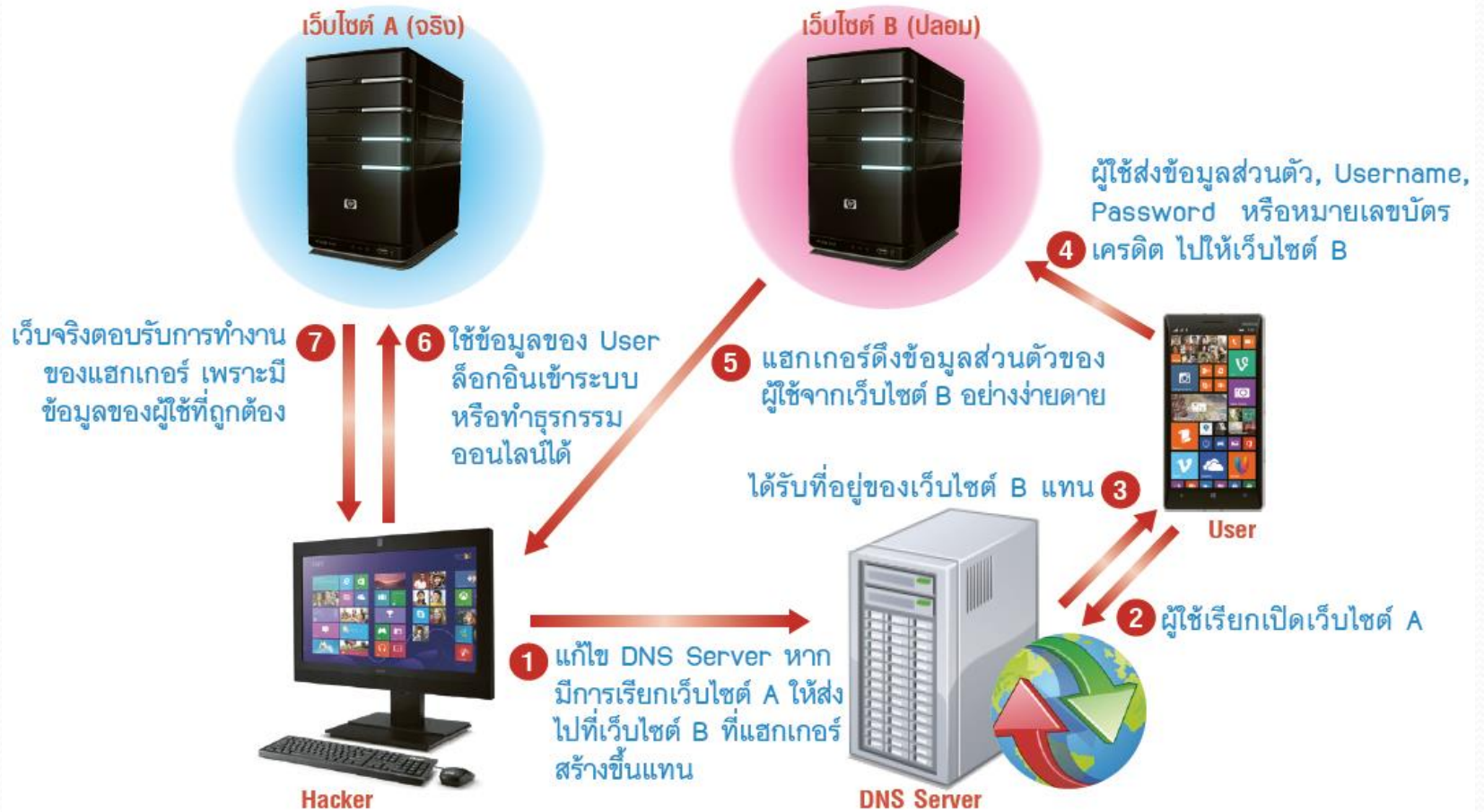
คุณต้องการติดตั้งแอปพลิเคชันที่เผยแพร่ในโทรศัพท์เคลื่อนที่ ซึ่งแอปพลิเคชันนี้ทำการรีเซ็ตและติดตั้งตัวรับรองความปลอดภัยของคุณโดยอัตโนมัติ การติดตั้ง เป็นเรื่องที่ไม่ยุ่งยาก เพียงครั้งเดียว ใช้เวลาไม่เกินกว่า 5 นาที.



ห้ามคลิก! ปุ่มใดๆ บนหน้าจอลอกหลวง



ตัวอย่าง Pharming

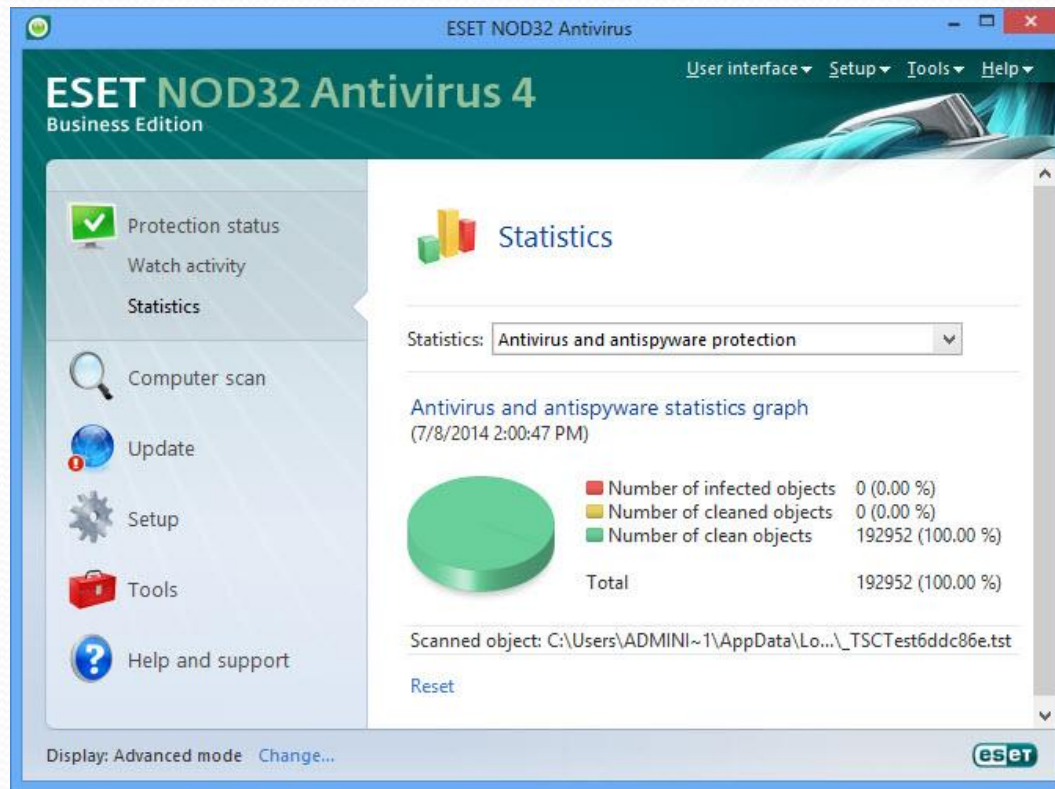




การรักษาความปลอดภัยระบบคอมพิวเตอร์

- การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus Program)
 - เปรียบเสมือนยามรักษาความปลอดภัยที่มาเฝ้าดูแลบ้าน
 - ทำหน้าที่คอยตรวจสอบและติดตามการบุกรุกของโปรแกรมประสงค์ร้าย เมื่อตรวจพบเจอก็สามารถกำจัดและแจ้งให้ผู้ใช้ทราบได้ทันที
 - ต้องหมั่นอัปเดตโปรแกรมให้มีข้อมูลใหม่ๆ อยู่เสมอ เพื่อให้ป้องกันไวรัสได้มีประสิทธิภาพ

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)



ตัวอย่างโปรแกรมป้องกันไวรัส ESET NOD32 Antivirus

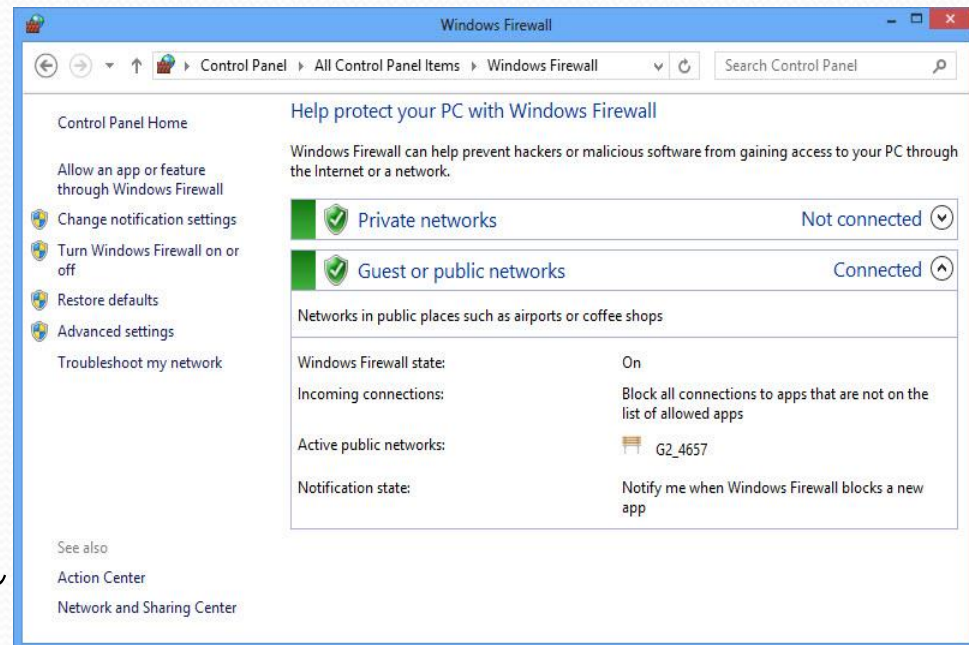
การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

- การใช้ระบบไฟร์วอลล์ (Firewall System)

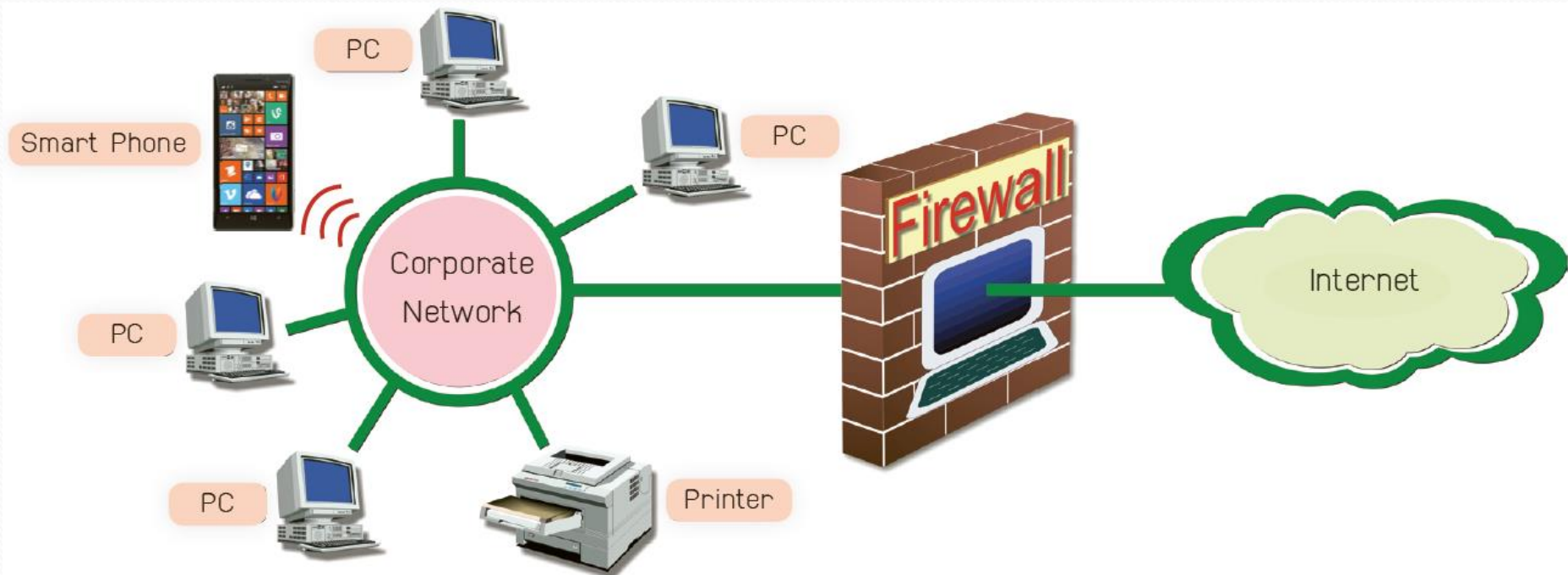
- เป็นระบบรักษาความปลอดภัยที่ประกอบด้วยฮาร์ดแวร์หรือซอฟต์แวร์ก็ได้

- ทำหน้าที่ดักจับ ป้องกันและตรวจสอบการบุกรุก (Intrusion) เข้าถึงระบบของผู้ไม่ประสงค์ดี

- ระบบจะให้ข้อมูลเฉพาะที่ได้รับ การอนุญาตผ่านเข้าออกเท่านั้น หากไม่ตรงกับเงื่อนไขข้อมูลนั้น จะไม่สามารถผ่านเข้าออกระบบได้



การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)



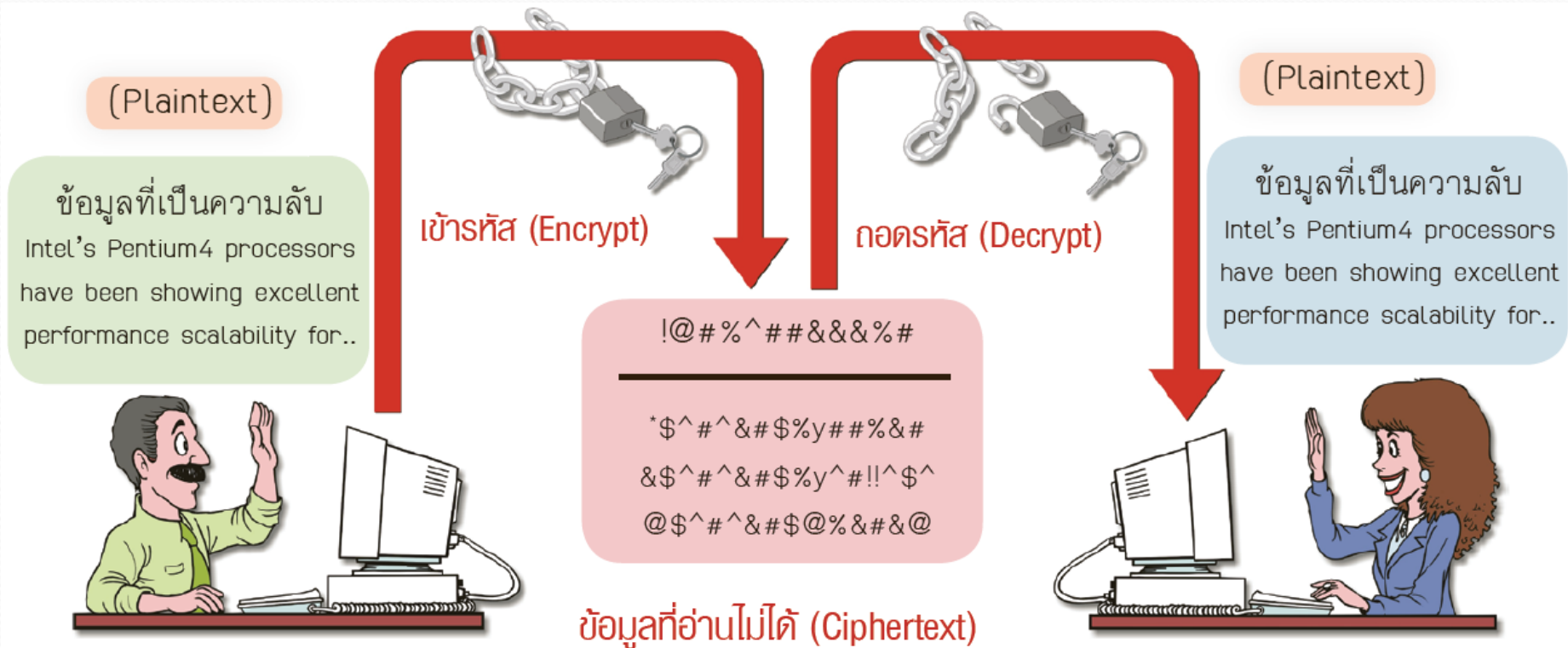
ภาพแสดงการติดตั้งระบบไฟร์วอลล์สำหรับเครือข่าย



การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

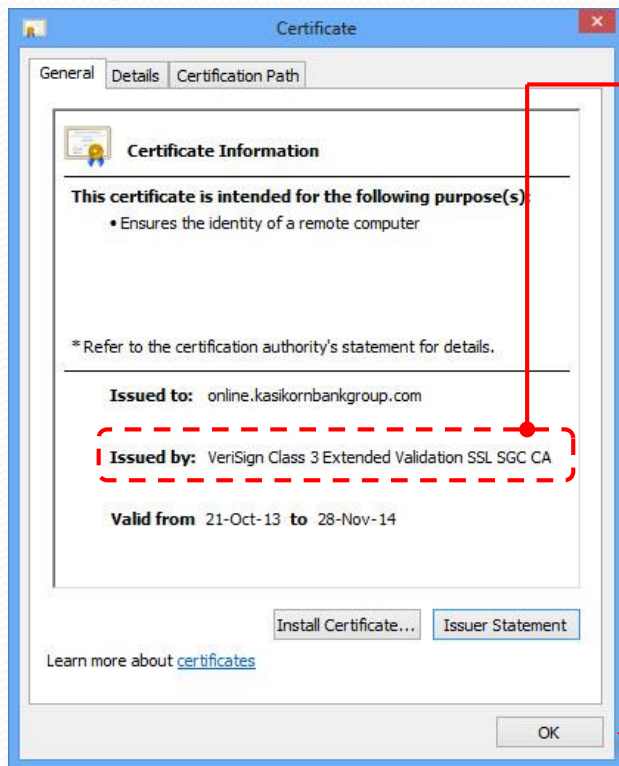
- **การเข้ารหัสข้อมูล (Encryption)**
 - อาศัยสมการทางคณิตศาสตร์ที่ซับซ้อน เพื่อเปลี่ยนแปลงข้อมูลที่สามารถอ่านได้ปกติ (Plaintext) ให้ไปอยู่ในรูปแบบที่ไม่สามารถอ่านได้ (Ciphertext)
 - ผู้ไม่ประสงค์ดีที่แอบเอาข้อมูลไปใช้ จะไม่สามารถอ่านข้อมูลที่มีความสำคัญนั้นได้ เพราะมีการเข้ารหัส (Encryption) ไว้
 - การอ่านข้อมูลนั้นจำเป็นต้องถอดรหัสข้อมูล (Decryption) ก่อน โดยใช้กุญแจ (Key) สำหรับไขอ่านข้อมูลนั้นๆ

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)



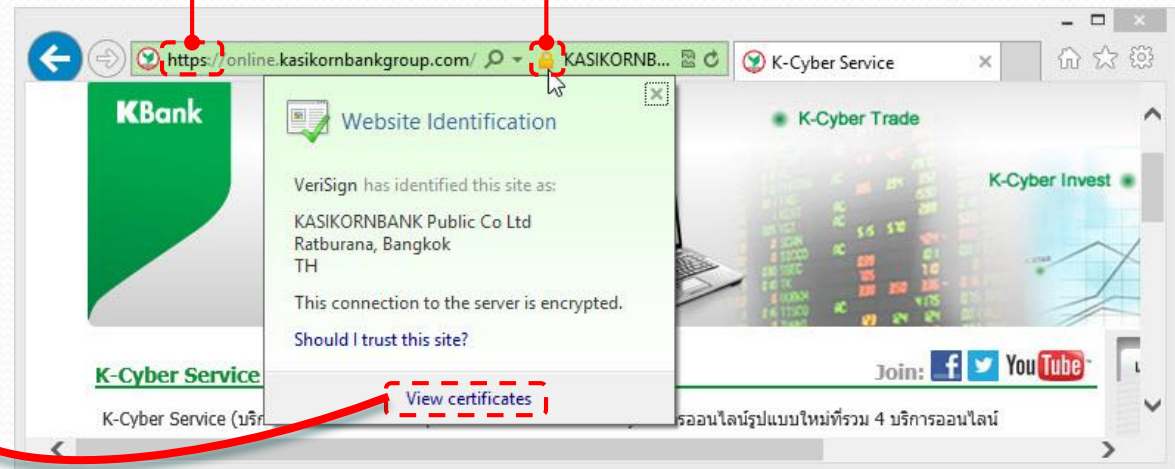
เทคนิคการเข้ารหัสและถอดรหัสของข้อมูล

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)



ผู้ออกใบรับรอง (Certificate)

แสดงถึงการเข้ารหัสความปลอดภัยบนเว็บนี้



ตัวอย่างหน้าเว็บที่มีการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูล

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

- การสำรองข้อมูล (Back up)

- คือการทำซ้ำข้อมูล ไฟล์ หรือโปรแกรมที่อยู่ในพื้นที่เก็บข้อมูล เพื่อให้สามารถนำกลับมาใช้ได้อีก กรณีที่ข้อมูลต้นฉบับนั้นเกิดสูญหายหรือถูกทำลาย
- วิธีการสำรองข้อมูลอาจทำทั้งระบบหรือแค่บางส่วน โดยเก็บลงหน่วยเก็บบันทึกข้อมูลสำรอง เช่น ฮาร์ดดิสก์, DVD หรือเทปบันทึกข้อมูล เป็นต้น
- หากข้อมูลมีความสำคัญมากอาจต้องสำรองข้อมูลทุกวัน หรือทุกสัปดาห์ แต่หากข้อมูลนั้นมีความสำคัญระดับทั่วไป ก็อาจสำรองข้อมูลเป็นรายเดือน



การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

- ความปลอดภัยบนสื่อสังคมออนไลน์
 - ภัยจากการใช้งาน เช่น ถูกผู้ไม่หวังดีแอบเจาะระบบบัญชี Social Media ของเรา แล้วขโมยข้อมูลไปใช้ได้
 - ภัยทางด้านสังคม เช่น ถูกหลอกลวงจากคนในสังคมออนไลน์ ทำให้เสียทรัพย์สิน เสียชื่อเสียง เกิดความไม่ปลอดภัยในชีวิต

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ใช้กำหนดมาตรการต่างๆ เพื่อควบคุมและเอาผิดกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยมีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม 2550 เป็นต้นไป เช่น
 - ทำลาย แก้ไข เปลี่ยนแปลง หรือทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเสียหาย
 - เข้าถึงข้อมูลคอมพิวเตอร์ หรือดักจับข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาต
 - ส่งต่ออีเมลที่มีข้อมูลไม่เหมาะสม เช่น ภาพ/คลิปหลุดที่ทำให้ผู้อื่นเสื่อมเสีย
 - ส่งข้อมูลรบกวนการใช้ระบบคอมพิวเตอร์ของคนอื่น
 - นำรหัสผ่านของผู้อื่นไปใช้แล้วเกิดความเสียหาย
 - โปสต์ข้อความแสดงความคิดเห็นโดยที่ไม่ไตร่ตรองให้ดี